John R. Parker, Jr,
California Bar No. 257761
ALMEIDA LAW GROUP LLC
3550 Watt Avenue, Suite 140
Sacramento, California 95821
Tel: (916) 616-2936
jrparker@almeidalawgroup.com

Attorneys for Plaintiff & the Proposed Class

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

Marie Catanach, *individually and on behalf of all others similarly situated,*

Plaintiff,

v.

Bold Quail Holdings, LLC, **Bold Quail 3, LLC**, **Bold Quail 3 Operations Holdings, LLC**, **NewGen, LLC**, and **NewGen Administrative Services, LLC**,

Defendants.

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT

Plaintiff Marie Catanach, individually and on behalf of all others similarly situated, by and through undersigned counsel, hereby alleges the following against Bold Quail Holdings, LLC, Bold Quail 3, LLC, Bold Quail 3 Operations Holdings, LLC, NewGen, LLC, and NewGen Administrative Services, LLC (collectively, "Defendants"). Facts pertaining to Plaintiff and her experiences and circumstances are alleged based upon personal knowledge and all other facts herein are alleged based upon the investigation of counsel and, where indicated, upon information and good faith belief.

NATURE OF THE ACTION

1. Plaintiff brings this class action lawsuit against Defendants for their failure to properly secure and safeguard Plaintiff's and other similarly situated current and former Defendants patients' (collectively defined herein as the "Class" or "Class Members") personally identifiable information ("PII") and protected health information ("PHI"), including names, dates of birth, Social Security numbers, Driver's licenses, health and health insurance information, and financial data (collectively, the "Private Information") from cybercriminals.

2. Bold Quail Holdings LLC is a Delaware limited liability company. Bold Quail 3, LLC, Bold Quail 3 Operations Holdings, LLC, NewGen LLC, and NewGen Administrative Services, LLC are California limited liability companies. On information and belief, these companies advise, operate, own, provide consulting services to, and provide information technology services to a network of rehabilitation, skilled nursing, behavioral health, and assisted living facilities on the West Coast, including, without limitation, S&F Market Street Healthcare, LLC; Windsor Care Center National City, Inc.; Windsor Cheviot Hills, LLC; Windsor Country Drive Care Center, LLC; Windsor Court Assisted Living, LLC; Windsor Cypress Gardens Healthcare, LLC; Windsor El Camino Care Center, LLC; Windsor Elk Grove and Rehabilitation Center, LLC; Windsor Elmhaven Care Center, LLC; Windsor Gardens Convalescent Hospital, Inc.; Windsor Hampton Care Center, LLC; Windsor Hayward Estates, LLC; Windsor Monterey Care Center, LLC; Windsor Rosewood Care Center, LLC; Windsor Sacramento Estates, LLC; Windsor Skyline Care Center, LLC; Windsor Terrace Healthcare, LLC; Windsor The Ridge Rehabilitation Center, LLC; and Windsor Vallejo Care Center, LLC, American River Center, Anaheim Terrace Care Center, Ballard Center, Bay Crest Care Center, Creekside Center, Devonshire Care Center, Fountain View Subacute and Nursing Center. Kingsburg Center, Linden Grove Health Care Center, Montebello Care Center, Montesano Health – Rehab Center, Orchard Park

Health Care and Rehab Center, Playa Del Rey Center, Rio Hondo Subacute and Nursing Center, Saint Joseph Transitional Rehabilitation Center, The Earlwood, The Heights of Summerlin, LLC, Willows Post Acute, and Woodland Care Center.

3. As part of their business, Defendants collect a treasure-trove of data from their patients, including highly sensitive Private Information.

4. Healthcare providers that handle Private Information have an obligation to employ reasonable and necessary data security practices to protect the sensitive, confidential and personal information entrusted to them.

5. This duty exists because it is foreseeable that the exposure of such Private Information to unauthorized persons—and especially hackers with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, medical and financial identity theft, invasion of their private health matters and other long-term issues.

6. The harm resulting from a data and privacy breach manifests in several ways, including identity theft and financial and medical fraud, and the exposure of a person's Private Information through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives.

7. Mitigating that risk—to the extent it is even possible to do so—requires individuals to devote significant time, money and other resources to closely monitor their credit, financial accounts, health records and email accounts, as well as to take a number of additional prophylactic measures.

8. In this instance, all of that could have been avoided if Defendants had employed reasonable and appropriate data security measures.

9. On February 23, 2024, Defendants announced that their patients' Private Information that had been entrusted to Defendants had been compromised in a "Hacking/IT incident," affecting at least 105,425 individuals (the "Data

Breach").[1]

10. This is one of the most egregious data breaches of recent years because it appears that the Data Breach took place *in September 2023 or even earlier* and in the months to come Defendants have gone to extraordinary lengths to conceal the details of the breach, including the number of affected victims and the exact categories of stolen data, until very recently.

11. The breach appears to have involved the divulgence of Private Information of Defendants' patients including their: name, address, diagnosis/conditions, lab results, medications, other treatment information, date of birth, driver's license and/or state identification number, Social Security number or other identifiers, claims information, credit card number, bank account number, and other financial information.

12. Thus, *despite discovering the Data Breach on or around September 14, 2023*, Defendants did not disclose the full scope of the Data Breach or the information impacted, until on or about February 23, 2024*, or over five months after the fact.* Moreover, Defendants failed to mount any meaningful investigation into the breach itself, the causes, or what specific information of Plaintiff and the proposed Class was lost to criminals.

13. Defendants' "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach has been severely diminished.

14. As a direct and proximate result of Defendants' failure to implement

[1] *See https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf* (last visited March 6, 2024).

and to follow basic security procedures, Plaintiff's and Class Members' PII and PHI is now in the hands of cybercriminals.

15. Plaintiff and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, misappropriation of health insurance benefits, intrusion of their health privacy and similar forms of criminal mischief, risk which may last for the rest of their lives.

16. Consequently, Plaintiff and Class Members must devote substantially more time, money and energy to protect themselves, to the extent possible, from these crimes. *See McMorris v. Lopez*, 995 F.3d 295, 301 (2d Cir. 2021) (quoting *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015) ("Why else would hackers break into a store's database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities.")).

17. Plaintiff, on behalf of herself and all others similarly situated, therefore brings claims for (i) Negligence; (ii) Negligence *per se*; (iii) Breach of Implied Contract; (iv) Unjust Enrichment; (vii) Violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq.*, (viii) Violation of the California Confidentiality of Medical Information Act, Cal. Civ. Code § 56, et. seq., and (ix) Declaratory Judgment. Plaintiff seeks damages and injunctive relief, including the adoption of reasonably necessary and appropriate data security practices to safeguard the Private Information in Defendants' custody in order to prevent incidents like the Data Breach from occurring in the future.

PARTIES

Plaintiff Catanach

18. Plaintiff Marie Catanach is, and at all times mentioned herein, was an individual citizen residing in Sacramento County, California, and was a patient of Defendants' facility called Windsor El Camino Care Services LLC in approximately September and August 2020.

19. Plaintiff understandably and reasonably believed and trusted that her Private Information provided to Defendants would be kept confidential and secure and would be used solely for authorized purposes.

Defendant Bold Quail Holdings LLC

20. Plaintiff is informed and believes that Defendant, Bold Quail Holdings, LLC, is a Delaware limited liability company that was at all times the 100% owner of Bold Quail 3 Operations Holdings, LLC.

21. Plaintiff is informed and believes that at all relevant times, the business address for Bold Quail Holdings, LLC, was 9526 West Pico Blvd., Los Angeles, CA 90035, the same address as Bold Quail 3 Operations Holdings, LLC. Plaintiff is informed and believes that as the owner of Bold Quail 3 Operations Holdings, LLC, Bold Quail Holdings, LLC was responsible for the day-to-day operations of a network of rehabilitation, skilled nursing, behavioral health, and assisted living facilities on the West Coast, including, without limitation, S&F Market Street Healthcare, LLC; Windsor Care Center National City, Inc.; Windsor Cheviot Hills, LLC; Windsor Country Drive Care Center, LLC; Windsor Court Assisted Living, LLC; Windsor Cypress Gardens Healthcare, LLC; Windsor El Camino Care Center, LLC; Windsor Elk Grove and Rehabilitation Center, LLC; Windsor Elmhaven Care Center, LLC; Windsor Gardens Convalescent Hospital, Inc.; Windsor Hampton Care Center, LLC; Windsor Hayward Estates, LLC; Windsor Monterey Care Center, LLC; Windsor Rosewood Care Center, LLC; Windsor Sacramento Estates, LLC; Windsor Skyline Care Center, LLC; Windsor Terrace Healthcare, LLC; Windsor The Ridge Rehabilitation Center, LLC; and Windsor Vallejo Care Center, LLC, American River Center, Anaheim Terrace Care Center, Ballard Center, Bay Crest Care Center, Creekside Center, Devonshire Care Center, Fountain View Subacute and Nursing Center. Kingsburg Center, Linden Grove Health Care Center, Montebello Care Center, Montesano Health – Rehab Center, Orchard Park Health Care and Rehab Center, Playa Del Rey Center,

Rio Hondo Subacute and Nursing Center, Saint Joseph Transitional Rehabilitation Center, The Earlwood, The Heights of Summerlin, LLC, Willows Post Acute, and Woodland Care Center.

Defendant Bold Quail 3 LLC

22. Defendant Bold Quail 3 LLC is a California limited liability company.

23. Plaintiff is informed and believes that at all relevant times, the business address for Bold Quail 3 LLC, was 9526 West Pico Blvd., Los Angeles, CA 90035, the same address as Bold Quail Holdings, LLC.

24. Plaintiff is informed and believes that at all relevant times Defendant Bold Quail 3 LLC was the parent organization of a network of rehabilitation, skilled nursing, behavioral health, and assisted living facilities on the West Coast, including, without limitation, S&F Market Street Healthcare, LLC; Windsor Care Center National City, Inc.; Windsor Cheviot Hills, LLC; Windsor Country Drive Care Center, LLC; Windsor Court Assisted Living, LLC; Windsor Cypress Gardens Healthcare, LLC; Windsor El Camino Care Center, LLC; Windsor Elk Grove and Rehabilitation Center, LLC; Windsor Elmhaven Care Center, LLC; Windsor Gardens Convalescent Hospital, Inc.; Windsor Hampton Care Center, LLC; Windsor Hayward Estates, LLC; Windsor Monterey Care Center, LLC; Windsor Rosewood Care Center, LLC; Windsor Sacramento Estates, LLC; Windsor Skyline Care Center, LLC; Windsor Terrace Healthcare, LLC; Windsor The Ridge Rehabilitation Center, LLC; and Windsor Vallejo Care Center, LLC, American River Center, Anaheim Terrace Care Center, Ballard Center, Bay Crest Care Center, Creekside Center, Devonshire Care Center, Fountain View Subacute and Nursing Center. Kingsburg Center, Linden Grove Health Care Center, Montebello Care Center, Montesano Health - Rehab Center, Orchard Park Health Care and Rehab Center, Playa Del Rey Center, Rio Hondo Subacute and Nursing Center, Saint Joseph Transitional Rehabilitation Center, The Earlwood, The Heights of Summerlin, LLC, Willows Post Acute, and Woodland Care Center.

Defendant Bold Quail 3 Operations Holdings LLC

25. Defendant Bold Quail 3 Operations Holdings LLC is a California limited liability company.

26. Plaintiff is informed and believes that at all relevant times, the business address for Bold Quail 3 Operations Holdings, LLC, was 9526 West Pico Blvd., Los Angeles, CA 90035, the same address as Bold Quail Holdings, LLC.

27. Plaintiff is informed and believes that at all relevant times Defendant Bold Quail 3 Operations Holdings, LLC was the parent organization of a network of rehabilitation, skilled nursing, behavioral health, and assisted living facilities on the West Coast, including, without limitation, S&F Market Street Healthcare, LLC; Windsor Care Center National City, Inc.; Windsor Cheviot Hills, LLC; Windsor Country Drive Care Center, LLC; Windsor Court Assisted Living, LLC; Windsor Cypress Gardens Healthcare, LLC; Windsor El Camino Care Center, LLC; Windsor Elk Grove and Rehabilitation Center, LLC; Windsor Elmhaven Care Center, LLC; Windsor Gardens Convalescent Hospital, Inc.; Windsor Hampton Care Center, LLC; Windsor Hayward Estates, LLC; Windsor Monterey Care Center, LLC; Windsor Rosewood Care Center, LLC; Windsor Sacramento Estates, LLC; Windsor Skyline Care Center, LLC; Windsor Terrace Healthcare, LLC; Windsor The Ridge Rehabilitation Center, LLC; and Windsor Vallejo Care Center, LLC, American River Center, Anaheim Terrace Care Center, Ballard Center, Bay Crest Care Center, Creekside Center, Devonshire Care Center, Fountain View Subacute and Nursing Center. Kingsburg Center, Linden Grove Health Care Center, Montebello Care Center, Montesano Health - Rehab Center, Orchard Park Health Care and Rehab Center, Playa Del Rey Center, Rio Hondo Subacute and Nursing Center, Saint Joseph Transitional Rehabilitation Center, The Earlwood, The Heights of Summerlin, LLC, Willows Post Acute, and Woodland Care Center.

Defendant NewGen LLC

28. Plaintiff is informed and believes that NewGen LLC is a California limited liability company, at all relevant times doing business at its principal place of business located at 9526 West Pico Blvd., Los Angeles, CA 90035, the same address of each other Defendant in this action, and was the management company for of a network of rehabilitation, skilled nursing, behavioral health, and assisted living facilities on the West Coast, including, without limitation, S&F Market Street Healthcare, LLC; Windsor Care Center National City, Inc.; Windsor Cheviot Hills, LLC; Windsor Country Drive Care Center, LLC; Windsor Court Assisted Living, LLC; Windsor Cypress Gardens Healthcare, LLC; Windsor El Camino Care Center, LLC; Windsor Elk Grove and Rehabilitation Center, LLC; Windsor Elmhaven Care Center, LLC; Windsor Gardens Convalescent Hospital, Inc.; Windsor Hampton Care Center, LLC; Windsor Hayward Estates, LLC; Windsor Monterey Care Center, LLC; Windsor Rosewood Care Center, LLC; Windsor Sacramento Estates, LLC; Windsor Skyline Care Center, LLC; Windsor Terrace Healthcare, LLC; Windsor The Ridge Rehabilitation Center, LLC; and Windsor Vallejo Care Center, LLC, American River Center, Anaheim Terrace Care Center, Ballard Center, Bay Crest Care Center, Creekside Center, Devonshire Care Center, Fountain View Subacute and Nursing Center. Kingsburg Center, Linden Grove Health Care Center, Montebello Care Center, Montesano Health - Rehab Center, Orchard Park Health Care and Rehab Center, Playa Del Rey Center, Rio Hondo Subacute and Nursing Center, Saint Joseph Transitional Rehabilitation Center, The Earlwood, The Heights of Summerlin, LLC, Willows Post Acute, and Woodland Care Center.

Defendant NewGen Administrative Services LLC

29. Plaintiff is informed and believes that NewGen Administrative Services, LLC is a California limited liability company, at all relevant times doing business at its principal place of business located at 9526 West Pico Blvd., Los Angeles, CA 90035, the same address of each other Defendant in this action, and was the management company for of a network of rehabilitation, skilled nursing, behavioral

health, and assisted living facilities on the West Coast, including, without limitation, S&F Market Street Healthcare, LLC; Windsor Care Center National City, Inc.; Windsor Cheviot Hills, LLC; Windsor Country Drive Care Center, LLC; Windsor Court Assisted Living, LLC; Windsor Cypress Gardens Healthcare, LLC; Windsor El Camino Care Center, LLC; Windsor Elk Grove and Rehabilitation Center, LLC; Windsor Elmhaven Care Center, LLC; Windsor Gardens Convalescent Hospital, Inc.; Windsor Hampton Care Center, LLC; Windsor Hayward Estates, LLC; Windsor Monterey Care Center, LLC; Windsor Rosewood Care Center, LLC; Windsor Sacramento Estates, LLC; Windsor Skyline Care Center, LLC; Windsor Terrace Healthcare, LLC; Windsor The Ridge Rehabilitation Center, LLC; and Windsor Vallejo Care Center, LLC, American River Center, Anaheim Terrace Care Center, Ballard Center, Bay Crest Care Center, Creekside Center, Devonshire Care Center, Fountain View Subacute and Nursing Center. Kingsburg Center, Linden Grove Health Care Center, Montebello Care Center, Montesano Health - Rehab Center, Orchard Park Health Care and Rehab Center, Playa Del Rey Center, Rio Hondo Subacute and Nursing Center, Saint Joseph Transitional Rehabilitation Center, The Earlwood, The Heights of Summerlin, LLC, Willows Post Acute, and Woodland Care Center.

JURISDICTION & VENUE

30. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than 100 putative class members and minimal diversity exists because Plaintiff and many putative class members are citizens of a different state than one or more Defendant.

31. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

32. This Court has personal jurisdiction over Defendants because they operate and maintain their principal place of business in this District. Further, Defendants are authorized to and regularly conduct business in this District and make decisions regarding corporate governance and management of their business operations in this District, including decisions regarding the security of patients' Private Information.

33. Venue is proper in this District under 28 U.S.C. § 1391(a)(1) through (d) because: a substantial part of the events giving rise to this action occurred in this District and Defendants have harmed Class Members residing in this District.

COMMON FACTUAL ALLEGATIONS

A. Defendants Collect a Significant Amount of Private Information.

34. Plaintiff is informed and believes that Defendants own, operate, and provide business and information technology support services to a network of rehabilitation, skilled nursing, behavioral health, and assisted living facilities on the West Coast, including, without limitation, S&F Market Street Healthcare, LLC; Windsor Care Center National City, Inc.; Windsor Cheviot Hills, LLC; Windsor Country Drive Care Center, LLC; Windsor Court Assisted Living, LLC; Windsor Cypress Gardens Healthcare, LLC; Windsor El Camino Care Center, LLC; Windsor Elk Grove and Rehabilitation Center, LLC; Windsor Elmhaven Care Center, LLC; Windsor Gardens Convalescent Hospital, Inc.; Windsor Hampton Care Center, LLC; Windsor Hayward Estates, LLC; Windsor Monterey Care Center, LLC; Windsor Rosewood Care Center, LLC; Windsor Sacramento Estates, LLC; Windsor Skyline Care Center, LLC; Windsor Terrace Healthcare, LLC; Windsor The Ridge Rehabilitation Center, LLC; and Windsor Vallejo Care Center, LLC, American River Center, Anaheim Terrace Care Center, Ballard Center, Bay Crest Care Center, Creekside Center, Devonshire Care Center, Fountain View Subacute and Nursing Center. Kingsburg Center, Linden Grove Health Care Center, Montebello Care Center, Montesano Health - Rehab Center, Orchard Park

Health Care and Rehab Center, Playa Del Rey Center, Rio Hondo Subacute and Nursing Center, Saint Joseph Transitional Rehabilitation Center, The Earlwood, The Heights of Summerlin, LLC, Willows Post Acute, and Woodland Care Center.

35. As a condition of receiving medical services from Defendants, patients are required to entrust them with highly sensitive personal and health information.

36. While providing healthcare services, Defendants receive, create and handle an incredible amount of Private Information, including, *inter alia*, names, addresses, dates of birth, addresses, phone numbers, email addresses, Social Security numbers and medical information such as dates of service, diagnosis/treatment information, medical billing/claims information, health insurance information and other information that Defendants may deem necessary to provide services and care.

37. Patients are required to provide and to otherwise entrust their PII and PHI to Defendants to receive healthcare services and, in return, they reasonably and appropriately expect that Defendants will safeguard their highly sensitive Private Information and keep it secure and confidential.

38. The information held by Defendants in their computer systems included the unencrypted Private Information of Plaintiff and Class Members.

39. Upon information and good faith belief, Defendants made promises and representations to their patients that the Private Information collected from them as a condition of obtaining healthcare services at Defendants' facilities would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendants would delete any sensitive information after they were no longer required to maintain it.

40. Due to the highly sensitive and personal nature of the information Defendants acquire and store with respect to their patients, Defendants are required to keep patients' Private Information private; comply with industry standards

related to data security and the maintenance of their patients' Private Information; inform their patients of its legal duties relating to data security and comply with all federal and state laws protecting patients' Private Information; only use and release patients' Private Information for reasons that relate to the services they provide; and provide adequate notice to patients if their Private Information is disclosed without authorization.

41. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendants assumed legal and equitable duties they owed to them and knew or should have known that they were responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure and exfiltration.

42. Without the required submission of Private Information from Plaintiff and Class Members, Defendants could not perform the services they provide.

43. Plaintiff and Class Members relied on Defendants to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendants ultimately failed to do.

44. Defendants' actions and inactions directly resulted in the Data Breach and the compromise of Plaintiff's and Class Members' Private Information.

B. Defendants Knew the Risks of Storing Valuable Private Information & the Foreseeable Harm to Victims.

45. Defendants were well aware that Private Information they collect is highly sensitive and of significant value to those who would use it for wrongful purposes.

46. Defendants also knew that a breach of their systems—and exposure of the information stored therein—would result in the increased risk of identity theft and fraud (financial and medical) against the individuals whose Private Information was compromised, as well as intrusion into their highly private health

information.

47. These risks are not merely theoretical; in recent years, numerous high-profile data breaches have occurred at businesses such as Equifax, Facebook, Yahoo, Marriott, Anthem as well as countless ones in the healthcare industry.

48. PII has considerable value and constitutes an enticing and well-known target to hackers, who can easily sell stolen data as there has been a "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[2]

49. PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.[3]

50. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses and government entities.

51. In 2021 alone, there were 4,145 publicly disclosed data breaches, exposing 22 billion records. The United States specifically saw a 10% increase in the total number of data breaches.[4]

52. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years; for instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million

---

[2] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/ (last visited March 6, 2024).

[3] *See* Brian O'Connor, *Healthcare Data Breach: What to Know About them and What to Do After One*, Experian (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last visited March 6, 2024).

[4] *Data Breach Report: 2021 Year End*, Risk Based Security (Feb. 4, 2022), https://www.riskbasedsecurity.com/2022/02/04/data-breach-report-2021-year-end/ (last visited March 6, 2024).

people in 2021.[5]

53. The healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[6]

54. Additionally, healthcare providers "store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it quickly – making the industry a growing target."[7]

55. Indeed, cybercriminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company Protenus found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[8]

56. The healthcare sector suffered about 337 breaches in the first half of 2022 alone according to Fortified Health Security's mid-year report released in July. The percentage of healthcare breaches attributed to malicious activity rose more than 5 percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[9]

---

[5] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20(last visited March 6, 2024).

[6] *The healthcare industry is at risk*, SwivelSecure https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited March 6, 2024).

[7] *Id.*

[8] *2022 Breach Barometer*, https://www.protenus.com/breach-barometer-report (last visited March 6, 2024).

[9] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half*

57. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendants' patients especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud and more.

58. As indicated by Jim Trainor, former second in command at the FBI's cyber security division: "[m]edical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70."[10]

59. A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market whereas stolen payment card information sells for about $1.[11] According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.
>
> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent

---

of Year, Cybersecurity News (July 19, 2022), https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year (last visited March 6, 2024).

[10] *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows*, IDX (May 14, 2015), https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat (last visited March 6, 2024).

[11] *Managing cyber risks in an interconnected world, Key findings from The Global State of Information Security® Survey 2015*, https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (last visited March 6, 2024).

> medical bills.
>
> Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[12]

60. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

61. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

---

[12] Brian O'Connor, *Healthcare Data Breach: What to Know About them and What to Do After One*, Experian (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last visited March 6, 2024).

62. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiff and Class Members.

63. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[13] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

64. Identity thieves can also use stolen personal information such as Social Security numbers and PHI for a variety of crimes, including medical identity theft, credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information.

65. For example, Social Security numbers, which were compromised in the Data Breach, are among the worst kind of Private Information to have been stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiffs and some Class Members, can lead to identity theft and extensive financial fraud:

---

[13] *See* https://www.identitytheft.gov/Steps (last visited March 6, 2024).

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[14]

66. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

67. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[15]

68. There may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or PHI is stolen and when it is misused.

69. According to the U.S. Government Accountability Office, which

---

[14] *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited March 6, 2024).

[15] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back* (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited March 6, 2024).

conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[16]

70. Even if stolen PII or PHI does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII and PHI about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

71. Based on the value of their patients' PII and PHI to cybercriminals, Defendants certainly knew the foreseeable risk of failing to implement adequate cybersecurity measures.

C. Defendants Breached their Duty to Protect their Patients' Private Information.

72. On February 23, 2024, Defendants announced that their patients' Private Information stored on their systems had been compromised in a "Hacking/IT incident," affecting 105,425 individuals (the "Data Breach").[17]

73. Defendants did not begin notifying patients impacted by the Data

---

[16] *Report to Congressional Requesters, Personal Information* (June 2007), https://www.gao.gov/new.items/d07737.pdf (last visited March 6, 2024).

[17] *See https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf* (last visited March 6, 2024).

Breach until *five months after they learned of the Data Breach*.

74. Even now Defendants still fail to disclose the true size of the Data Breach, refusing to provide the number of affected victims, when the Data Breach took place, and what exact types of information have been stolen by cyber criminals.

75. The Data Breach occurred as a direct result of Defendants' failure to implement and follow basic security procedures, and its failure to follow their own policies, in order to protect their patients' PII and PHI.

D. Defendants are Obligated Under HIPAA to Safeguard Private Information.

76. Defendants are required by HIPAA to safeguard patient PHI.

77. Defendants are entitities covered under HIPAA, which sets minimum federal standards for privacy and security of PHI.

78. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

79. Further to 45 C.F.R. § 160.103, HIPAA defines "protected health information" or PHI as "individually identifiable health information" that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium."

80. Under C.F.R. 160.103, HIPAA defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2)"[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and (3) either (a) identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the

individual."

81. HIPAA requires Defendants to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA's security requirements. 45 CFR § 164.102, *et. seq*.

82. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendantsto provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."[18]

83. While HIPAA permits healthcare providers to disclose PHI to third parties under certain circumstances, HIPAA does not permit healthcare providers to disclose PHI to cybercriminals nor did Plaintiff or the Class Members consent to the disclosure of their PHI to cybercriminals.

84. As such, Defendants are required under HIPAA to maintain the strictest confidentiality of Plaintiff's and Class Members' PHI that it requires, receives, and collects, and Defendants are further required to maintain sufficient safeguards to protect that information from being accessed by unauthorized third parties.

85. Given the application of HIPAA to Defendants, and that Plaintiff and Class Members entrusted their PHI to Defendants in order to receive healthcare services, Plaintiff and Class Members reasonably expected that Defendants would safeguard their highly sensitive information and keep their PHI confidential.

E. FTC Guidelines Prohibit Defendants from Engaging in Unfair or

[18] *Breach Notification Rule*, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

Deceptive Acts or Practices.

86. Defendants are prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

87. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[19]

88. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[20]

89. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[21]

90. The FTC has brought enforcement actions against businesses for

[19] *Start with Security – A Guide for Business* (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited March 6, 2024)

[20] *Protecting Personal Information: A Guide for Business*, United States Federal Trade Comm'n, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited March 6, 2024)

[21] *Id.*

failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

91. Defendants failed to properly implement basic data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII and PHI constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

92. Defendants were at all times fully aware of their obligations to protect the PII and PHI of patients because of their position as healthcare providers, which gave them direct access to reams of patient PII and PHI. Defendants were also aware of the significant repercussions that would result from their failure to do so.

F. The Monetary Value of Private Information.

93. As a result of Defendants' failures, Plaintiff and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of their Private Information.

94. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud—this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[22]

95. With respect to health care breaches, another study found "the majority [70%] of data impacted by healthcare breaches could be leveraged by

[22] Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud (last visited March 6, 2024).

hackers to commit fraud or identity theft."[23]

96. "Actors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[24]

97. The reality is that cybercriminals seek nefarious outcomes from a data breach and "stolen health data can be used to carry out a variety of crimes."[25]

98. Indeed, a robust "cyber black market" exists in which criminals openly post stolen Private Information on multiple underground Internet websites, commonly referred to as the dark web.

99. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third-party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[26]

---

[23] Jessica David, *70% of Data Involved in Healthcare Breaches Increases Risk of Fraud*, https://healthitsecurity.com/news/70-of-data-involved-in-healthcare-breachesincreases-risk-of-fraud (last visited March 6, 2024).

[24] *Id.*

[25] Andrew Steger, *What Happens to Stolen Healthcare Data?* (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last visited March 6, 2024).

[26] *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data*, at 8:2-8 (Mar. 13, 2001), https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf (last visited March 6, 2024).

100. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 Billion per year online advertising industry in the United States.[27]

101. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[28]

102. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[29] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

103. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how

---

[27] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy* (Feb. 28, 2011), https://www.wsj.com/articles/SB10001424052748703529004576160764037920274 (last visited March 6, 2024).

[28] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable* (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf (last visited March 6, 2024).

[29] Angwin & Steel, *supra* note 27.

much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[30]

104. The value of Plaintiff's and Class Members' Private Information on the black market is substantial. Sensitive health information can sell for as much as $363.[31]

105. This information is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

106. Health information in particular is likely to be used in detrimental ways—by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.[32]

107. "Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft. Additionally, medical identity theft is very difficult to detect which makes this form of fraud extremely dangerous."[33]

108. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's

---

[30] *See* U.S. Dep't of Justice, *Victims of Identity Theft,* OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited March 6, 2024).

[31] *Data Breaches: In the Healthcare Sector*, https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (last visited March 6, 2024).

[32] *Id.*

[33] *The Potential Damages and Consequences of Medical Identity theft and Healthcare Data Breaches*, https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last visited March 6, 2024).

health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[34]

109. The Federal Trade Commission has warned consumers of the dangers of medical identity theft, stating that criminals can use personal information like a "health insurance account number or Medicare number" to "see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." The FTC further warns that instances of medical identity theft "could affect the medical care you're able to get or the health insurance benefits you're able to use[,]" while also having a negative impact on credit scores.[35]

110. Here, where health insurance information was among the Private Information impacted in the Data Breach, Plaintiff's and Class Members' risk of suffering future medical identity theft is especially substantial.[36]

111. The ramifications of Defendants' failure to keep their patients' Private Information secure are long-lasting and severe. Once Private Information is stolen,

---

[34] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER (Feb. 7, 2014) https://khn.org/news/rise-of-indentity-theft/ (last visited March 6, 2024).

[35] *What to Know About Medical Identity Theft*, What To Know About Medical Identity Theft | Consumer Advice (ftc.gov) (last visited March 6, 2024).

[36] *See Watch for Medical Identity Theft*, https://www.aarp.org/money/scams-fraud/info-11-2010/watch_for_medical_wy.html#:~:text=Medical%20identity%20theft%20is%20when%20someone%20uses%20your,You%20can%20be%20harmed%20by%20medical%20identity%20theft (last visited March 6, 2024).

fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for 6 to 12 months or even longer.

112. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened.[37] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[38]

113. Indeed, when compromised, healthcare related data is among the most private and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[39]

114. Almost 50% of the surveyed victims lost their healthcare coverage as a result of the incident, while nearly 30% said their insurance premiums went up after the event. Forty percent of the victims were never able to resolve their identity theft at all. Seventy-four percent said that the effort to resolve the crime and restore their identity was significant or very significant. Data breaches and identity theft, including medical identity theft, have a crippling effect on

---

[37] *See Medical ID Theft Checklist*, IDENTITYFORCE, https://www.identityforce.com/blog/medical-id-theft-checklist-2 (last visited March 6, 2024).

[38] *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches* (Apr. 2010), https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last visited March 6, 2024).

[39] Elinor Mills, *Study: Medical identity theft is costly for victims* (March 3, 2010), https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/ (last visited March 6, 2024).

individuals and detrimentally impact the economy as a whole.[40]

115. At all relevant times, Defendants were well-aware, or reasonably should have been aware, that the Private Information they maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft (including medical identity theft) and fraud.

116. Upon information and good faith belief, had Defendants remedied the deficiencies in their security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, they would have prevented the ransomware attack into their systems and, ultimately, the theft of the Private Information of patients within their systems.

117. The compromised Private Information in the Data Breach is of great value to hackers and thieves and can be used in a variety of ways. Information about, or related to, an individual for which there is a possibility of logical association with other information is of great value to hackers and thieves.

118. Indeed, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[41] For example, different PII elements from various sources may be able to be linked in order to identify an individual, or access additional information about or relating to the individual.[42]

---

[40] *Id.*

[41] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report*, at 35-38 (Dec. 2010), https://www.ftc.gov/reports/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework (last visited March 6, 2024).

[42] *See id.* (evaluating privacy framework for entities collecting or using consumer

119. Based upon information and belief, the unauthorized parties have already utilized, and will continue utilize, the Private Information they obtained through the Data Breach to obtain additional information from Plaintiff and Class Members that can be misused.

120. In addition, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

121. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

122. Thus, even if payment card information were not involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access accounts, including, but not limited to email accounts and financial accounts, to engage in the fraudulent activity identified by Plaintiffs.

123. Given these facts, any company that transacts business with customers and then compromises the privacy of customers' Private Information has thus deprived customers of the full monetary value of their transaction with the company.

124. In short, the Private Information exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breach can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names.

G. Plaintiff & Class Members Have Suffered Compensable Damages.

125. For the reasons mentioned above, Defendants' conduct, which

---

data with can be "reasonably linked to a specific consumer, computer, or other device").

allowed the Data Breach to occur, caused Plaintiff and Class Members significant injuries and harm in several ways.

126. The risks associated with identity theft, including medical identity theft, are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds to thousands of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

127. In order to mitigate against the risks of identity theft and fraud, Plaintiff and members of the Class must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

128. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendants' conduct.

129. Further, the value of Plaintiff and Class Members' PII and PHI has been diminished by its exposure in the Data Breach.

130. Plaintiff and Class Members now face a greater risk of identity theft, including medical and financial identity theft.

131. Plaintiff and Class Members are also at a continued risk because their

information remains in Defendants' systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Defendantsfail to undertake the necessary and appropriate security and training measures to protect their patients' PII and PHI.

132. Plaintiff and Class Members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private medical information to strangers.

133. Plaintiff and Class Members also did not receive the full benefit of their bargain when paying for medical services. Instead, they received services of a diminished value to those described in their agreements with Defendants. Plaintiff and Class Members were damaged in an amount at least equal to the difference in the value between the services they thought they paid for (which would have included adequate data security protection) and the services they actually received.

134. Plaintiff and Class Members would not have obtained services from Defendants had they known that Defendants failed to properly train their employees, lacked safety controls over their computer network, and did not have proper data security practices to safeguard their Private Information from criminal theft and misuse.

135. Finally, in addition to a remedy for the economic harm, Plaintiff and Class Members maintain an undeniable interest in ensuring that their Private Information remains secure and is not subject to further misappropriation and theft.

REPRESENTATIVE PLAINTIFF'S EXPERIENCE

Plaintiff Catanach

136. Beginning in or around August 2022, Plaintiff Catanach was a patient at one of Defendants' facilities.

137. As a patient, Defendants required Plaintiff to provide—and Plaintiff provided—Private Information including her first and last name, birth date, email address, phone number and reason for visit, as well as her social security number,

insurance information, and payment information.

138. As a direct result of the Data Breach, Plaintiff has suffered or will imminently suffer injury from the unauthorized disclosure and misuse of her Private Information that can be directly traced to Defendants.

139. On information and belief, Plaintiff's Private Information unauthorizedly disclosed in the Data Breach is now in the possession of cybercriminals and/or on the Dark Web where it can be sold and utilized for fraudulent and criminal purposes.

140. In addition, Plaintiff must now spend time and effort attempting to remediate the harmful effects of the Data Breach, including monitoring their credit reports, and fears for their personal financial security and uncertainty over the information compromised in the Data Breach. She is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

141. Plaintiff was highly disturbed by the Data Breach's nature and the thought of cybercriminals accessing her highly sensitive Private Information and the harm caused by the Data Breach.

142. As a result of Defendants' Data Breach, Plaintiff faces a lifetime risk of additional identity theft, because it includes sensitive information that cannot be changed, like her Social Security number.

CLASS ALLEGATIONS

143. Plaintiff brings this class action on behalf of herself and all other individuals who are similarly situated pursuant to Rule 23 of the Federal Rules of Civil Procedure.

144. Plaintiff seeks to represent a Nationwide Class of persons to be defined as follows:

All individuals in the United States whose PII and/or PHI was

compromised in the Defendants' Data Breach which occurred in or about 2023 and was announced in February 2024 (the "Nationwide Class").

145. In addition, or in the alternative, Plaintiff proposes the following California Sub-Class definition, subject to amendment as appropriate (together with the Nationwide Class, the "Class"):

All California residents whose PII and/or PHI was compromised in the Defendants' Data Breach which occurred in or about 2023 and was announced in February 2024 (the "California Sub-Class").

146. Excluded from the Class are Defendants, their subsidiaries and affiliates, officers and directors, any entity in which Defendants have a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

147. This proposed class definition is based on the information available to Plaintiff at this time. Plaintiff may modify the class definition in an amended pleading or when she moves for class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

148. **Numerosity:** Plaintiff is informed and believes, and thereon alleges, that there are at minimum, thousands of members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through Defendants' records, including but not limited to the files implicated in the Data Breach, but based on public information, the Class includes thousands of individuals, if not substantially more.

149. **Commonality:** This action involved questions of law and fact common to the Class. Such common questions include but are not limited to:

a. Whether Defendants failed to timely notify Plaintiff and Class Members of the Data Breach;

b. Whether Defendants had a duty to protect the PII and PHI of Plaintiff and Class Members;

c. Whether Defendants were negligent in collecting and storing Plaintiff's and Class Members' PII and PHI, and breached their duties thereby;

d. Whether Defendants entered into an implied contract with Plaintiff and Class Members;

e. Whether Defendants breached that contract by failing to adequately safeguard Plaintiff's and Class Members' PII and PHI;

f. Whether Defendants were unjustly enriched;

g. Whether Plaintiff and Class Members are entitled to damages as a result of Defendants' wrongful conduct; and

h. Whether Plaintiff and Class Members are entitled to declaratory judgment due to Defendants' wrongful conduct.

150. **Typicality:** Plaintiff's claims are typical of the claims of the members of the Class. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiff and members of the Class were all patients, or family members or caregivers of patients, of Defendants, each having their PII and PHI exposed and/or accessed by an unauthorized third party.

151. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the members of the Class. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of the members of the Class and have no interests antagonistic to the members of the Class. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff and the Class Members are substantially identical as explained above.

152. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense, and promote uniform decision-making.

153. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendants' liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendants breached their duty to Plaintiff and Class Members, then Plaintiff and each Class member suffered damages by that conduct.

154. **Injunctive Relief:** Defendants have acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

155. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria and Class Members may be readily identified through Defendants' books and records.

CALIFORNIA LAW SHOULD APPLY TO PLAINTIFF'S & CLASS MEMBERS' COMMON LAW CLAIMS

156. The State of California has a significant interest in regulating the conduct of businesses operating within its borders.

157. The State of California has a significant interest in regulating the conduct of businesses operating within its borders.

158. California, which seeks to protect the rights and interests of California and all residents and citizens of the United States against a company headquartered and doing business in California, has a greater interest in the claims of Plaintiff and the Classes than any other state and is most intimately concerned with the claims and outcome of this litigation.

159. The principal place of business and headquarters of Defendants, located in California, is the "nerve center" of its business activities—the place where their high-level officers direct, control and coordinate their activities, including major policy, financial and legal decisions.

160. Upon information and good faith belief, Defendants' actions and corporate decisions surrounding the allegations made in the Complaint were made from and in California.

161. Defendants' breaches of duty to Plaintiff and Class Members emanated from California.

162. Application of California law to the Classes with respect to Plaintiff's and the Classes' common law claims is neither arbitrary nor fundamentally unfair because, further to choice of law principles applicable to this action, the common law of California applies to the nationwide common law claims of all Class members. Additionally, given California' significant interest in regulating the conduct of businesses operating within its borders, and that California has the most significant relationship to Defendants, as most of them are headquartered and incorporated in California, and all of them are located in and doing business there, there is no conflict in applying California law to non-resident consumers such as Plaintiff and Class Members. Alternatively, and/or in addition to California law, the laws set forth below apply to the conduct described herein.

CAUSES OF ACTION

COUNT I

Negligence

(On behalf of Plaintiff & the Nationwide Class)

163. Plaintiff restates and realleges all preceding factual allegations above as if fully set forth herein.

164. Plaintiff brings this claim individually and on behalf of the Class.

165. Defendants owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII and PHI in Defendants' possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

166. Defendants' duty to use reasonable care arose from several sources, including but not limited to those described below.

167. Defendants had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of the Defendants. By collecting and storing valuable PII and PHI that is routinely targeted by criminals for unauthorized access, Defendants were obligated to act with reasonable care to protect against these foreseeable threats.

168. Defendants' duty also arose from Defendants' position as healthcare providers. Defendants hold themselves out as trusted providers of healthcare, and thereby assume a duty to reasonably protect their patients' information. Indeed, Defendants were in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

169. Defendants breached the duties owed to Plaintiff and Class Members and thus were negligent. As a result of a successful attack directed towards Defendants that compromised Plaintiff's and Class Members' PII and PHI, Defendants breached their duties through some combination of the following errors and omissions that allowed the data compromise to occur: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to

the security, confidentiality, and integrity of patient information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust their information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow their own privacy policies and practices published to their patients; and (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII or PHI.

170. But for Defendants' wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII and PHI would not have been compromised.

171. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII and/or PHI;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by

their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data;

i. Future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members;

j. The diminished value of the services they paid for and received, and

k. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

172. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT II

Negligence *Per Se*

(On behalf of Plaintiff & the Nationwide Class)

173. Plaintiff restates and realleges all preceding factual allegations above as if fully set forth herein.

174. Plaintiff brings this claim individually and on behalf of the Class.

175. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Defendantsor failing to use reasonable measures to protect PII and PHI. Various FTC publications and orders also form the basis of Defendants' duty.

176. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with the industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII and PHI they obtained and stored and the foreseeable consequences of a data breach involving PII and PHI of their patients.

177. Plaintiff and members of the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

178. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

179. Defendants are entities covered under HIPAA which sets minimum federal standards for privacy and security of PHI.

180. Pursuant to HIPAA, 42 U.S.C. § 1302d, *et. seq.*, and its implementing regulations, Defendants had a duty to implement and maintain reasonable and appropriate administrative, technical, and physical safeguards to protect Plaintiff's and the Class Members' electronic PHI.

181. Specifically, HIPAA required Defendants to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by their workforce to satisfy HIPAA's security requirements. 45 C.F.R. § 164.102, *et. seq*.

182. Defendants violated HIPAA by actively disclosing Plaintiff's and the Class Members' electronic PHI and by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PHI.

183. Plaintiff and the Class Members are patients within the class of persons HIPAA was intended to protect.

184. Defendants' violation of HIPAA constitutes negligence *per se*.

185. The harm that has occurred as a result of Defendants' conduct is the type of harm that the FTC Act and HIPAA were intended to guard against.

186. As a direct and proximate result of Defendants' negligence, Plaintiff's and Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

187. Upon accepting, storing, and controlling the Private Information of Plaintiff and the Class, Defendants owed, and continue to owe, a duty to Plaintiff and the Class to exercise reasonable care to secure, safeguard and protect their highly sensitive Private Information.

188. Defendants breached this duty by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

189. Defendants' duty of care to use reasonable measures to secure and safeguard Plaintiff's and Class Members' Private Information arose due to the special relationship that existed between Defendants and their facilities' patients, which is recognized by statute, regulations, and the common law.

190. In addition, Defendants had a duty under HIPAA privacy laws, which were enacted with the objective of protecting the confidentiality of clients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

191. Defendants' own conduct also created a foreseeable risk of harm to Plaintiff and Class Members and their Private Information. Defendants'

misconduct included the failure to (1) secure Plaintiff's and Class Members' Private Information and (2) comply with industry-standard data security practices.

192. As a direct result of Defendants' breach of their duty of confidentiality and privacy and the disclosure of Plaintiff's and Class Members' Private Information, Plaintiff and the Class have suffered damages that include, without limitation, loss of the benefit of the bargain, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

193. Defendants' wrongful actions and/or inactions and the resulting unauthorized disclosure of Plaintiff's and Class Members' Private Information constituted (and continue to constitute) negligence at common law.

194. Plaintiff and the Class are entitled to recover damages in an amount to be determined at trial.

COUNT III

Breach of Implied Contract

(On behalf of Plaintiff & the Nationwide Class)

195. Plaintiff restates and realleges all preceding factual allegations above as if fully set forth herein.

196. Plaintiff brings this claim individually and on behalf of the Class.

197. When Plaintiff and Class Members provided their PII and PHI to Defendants, they entered into implied contracts with Defendants, under which Defendants agreed to take reasonable steps to protect Plaintiff's and Class Members' PII and PHI, comply with their statutory and common law duties to protect Plaintiff's and Class Members' PII and PHI, and to timely notify them in the event of a data breach.

198. Defendants solicited and invited Plaintiff and Class Members to provide their PII and PHI as part of Defendants' provision of healthcare services. Plaintiff and Class Members accepted Defendants' offers and provided their PII and PHI to Defendants.

199. Implicit in the agreement between Plaintiff and Class Members and Defendants, was Defendants' obligation to: (a) use such PII and PHI for business purposes only; (b) take reasonable steps to safeguard Plaintiff's and Class Members' PII and PHI; (c) prevent unauthorized access and/or disclosure of Plaintiff's and Class Members' PII and PHI; (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or disclosure of their PII and PHI; (e) reasonably safeguard and protect the PII and PHI of Plaintiff and Class Members from unauthorized access and/or disclosure; and (f) retain Plaintiff's and Class Members' PII and PHI under conditions that kept such information secure and confidential.

200. When entering into implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendants' data security practices complied with their statutory and common law duties to adequately protect Plaintiff's and Class Members' PII and PHI and to timely notify them in the event of a data breach.

201. Plaintiff and Class Members paid money to Defendants in exchange for services, along with Defendants' promise to protect their PII and PHI from unauthorized access and disclosure. Plaintiff and Class Members reasonably believed and expected that Defendants would use part of those funds to obtain adequate data security. Defendants failed to do so.

202. Plaintiff and Class Members would not have provided their PII and PHI to Defendants had they known that Defendants would not safeguard their PII and PHI, as promised, or provide timely notice of a data breach.

203. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendants.

204. Defendants breached its implied contracts with Plaintiff and Class Members by failing to safeguard their PII and PHI and by failing to provide them with timely and accurate notice of the Data Breach

205. The losses and damages Plaintiff and Class Members sustained, include, but are not limited to:

a. Theft of their PII and/or PHI;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII and PHI;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data;

i. Future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members;

j. The diminished value of the services they paid for and received; and

k. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

206. As a direct and proximate result of Defendants' breach of contract,

Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

207. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, *e.g.*, (1) strength their data security systems and monitoring procedures; (2) submit to future annual audits of those systems and monitoring procedures; and (3) immediately provide and continue to provide adequate credit monitoring to Plaintiff and all Class Members.

COUNT IV

Unjust Enrichment

(*On behalf of Plaintiff & the Nationwide Class*)

208. Plaintiff restates and realleges all preceding factual allegations above as if fully set forth herein.

209. Plaintiff brings this claim individually and on behalf of the Class.

210. Upon information and belief, Defendants fund their data security measures from their general revenue including payments made by or on behalf of Plaintiff and Class Members.

211. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendants.

212. Plaintiff and Class Members conferred a monetary benefit on Defendants. Specifically, they purchased healthcare services from Defendants and/or their agents and in so doing provided Defendants with their PII and PHI.

213. In exchange, Plaintiff and Class Members should have received from Defendants the goods and services that were the subject of the transaction and have their PII and PHI protected with adequate data security.

214. Defendants knew that Plaintiff and Class Members conferred a benefit which Defendants accepted. Defendants profited from these transactions and used

the PII and PHI of Plaintiff and Class Members for business purposes.

215. In particular, Defendants enriched themselves by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members PII and PHI. Instead of providing a reasonable level of data security that would have prevented the Data Breach, Defendants instead calculated to increase their own profits and the expense of Plaintiff and Class Members by utilizing cheaper, ineffective data security measures.

216. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendants failed to implement appropriate data management and security measures that are mandated by their common law and statutory duties.

217. Defendants failed to secure Plaintiff and Class Members' PII and PHI and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members conferred upon Defendants.

218. Defendants acquired Plaintiff's and Class Members' PII and PHI through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

219. If Plaintiff and Class Members knew that Defendants had not reasonably secured their PII and PHI, they would not have agreed to provide their PII and PHI to Defendants.

220. Plaintiff and Class Members have no adequate remedy at law.

221. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII and/or PHI;
b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;
c. Costs associated with purchasing credit monitoring and identity theft protection services;
d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' data;

i. Future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members;

j. The diminished value of the services they paid for and received; and

k. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

222. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and noneconomic losses.

223. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendants should be

compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendants' services.

COUNT V

California Confidentiality of Medical Information Act,

Civil Code §§ 56, *et seq*.

(On behalf of Plaintiff & the California Class)

224. Plaintiff restates and realleges all preceding factual allegations above as if fully set forth herein.

225. Under the California Confidentiality of Medical Information Act, Civil Code §§ 56, *et seq*. (hereinafter referred to as the "CMIA"), "medical information" means "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment." Cal. Civ. Code § 56.05.

226. Additionally, Cal. Civ. Code § 56.05 defines "individually identifiable" as meaning that "the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the identity of the individual." Cal. Civ. Code § 56.05.

227. Under Cal. Civ. Code § 56.101(a) of the CMIA,

> (a) Every provider of health care, health care service plan, pharmaceutical company, or contractor who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein.

> Any provider of health care, health care service plan, pharmaceutical company, or contractor who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36.
>
> Cal. Civ. Code § 56.101.

228. At all relevant times, Defendants were health care contractors within the meaning of Civil Code § 56.05(d) because they are each and collectively a "medical group, independent practice association, pharmaceutical benefits manager, or medical service organization and is not a health care service plan or provider of health care." In the alternative, Defendants are health care providers within the meaning of Civil Code § 56.06(b) because it maintains medical information as defined by Civil Code § 56.05.

229. Plaintiff and Class Members are Defendants' patients, as defined in Civil Code § 56.05(k).

230. Plaintiff and Class Members provided their personal medical information to Defendants.

231. At all relevant times, Defendants created, maintained, preserved, stored, abandoned, destroyed, or disposed of medical information in the ordinary course business.

232. As a result of the Data Breach, Defendants have misused, disclosed, and/or allowed third parties to access and view Plaintiff's and Class Members' personal medical information without their written authorization compliant with the provisions of Civil Code §§ 56, et seq. As a further result of the Data Breach, the confidential nature of the plaintiff's medical information was breached as a result of Defendants' negligence. Specifically, Defendants knowingly allowed and affirmatively acted in a manner that actually allowed unauthorized parties to access and view Plaintiff's and Class Members' Private Information, which was

viewed and used when the unauthorized parties engaged in the above-described fraudulent activity. Defendants' misuse and/or disclosure of medical information regarding Plaintiff and Class Members constitutes a violation of Civil Code §§ 56.10, 56.11, 56.13, and 56.26.

233. As a direct and proximate result of Defendants' wrongful actions, inaction, omissions, and want of ordinary care, Plaintiff's and Class Members' personal medical information was disclosed without written authorization.

234. By disclosing Plaintiff's and Class Members' Private Information without their written authorization, Defendants violated California Civil Code § 56, et seq., and their legal duty to protect the confidentiality of such information.

235. Defendants also violated Sections 56.06 and 56.101 of the California CMIA, which prohibit the negligent creation, maintenance, preservation, storage, abandonment, destruction or disposal of confidential personal medical information.

236. As a direct and proximate result of Defendants' wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff's and Class Members' personal medical information was viewed by, released to, and disclosed to third parties without Plaintiff's and Class Members' written authorization.

As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violation of the CMIA, Plaintiff and Class Members are entitled to (i) actual damages, (ii) nominal damages of $1,000 per Plaintiff and Class Member, (iii) punitive damages of up to $3,000 per Plaintiff and Class Member, and (iv) attorneys' fees, litigation expenses and court costs under California Civil Code § 56.35.

COUNT VI

California Unfair Competition Law

Cal. Bus. & Prof. Code §17200 *et seq*.

(On Behalf of Plaintiff and the Nationwide Class)

237. Plaintiff re-alleges and incorporates by reference each and every allegation in this Complaint, as if fully set forth herein.

238. Defendants are "persons" defined by Cal. Bus. & Prof. Code § 17201.

239. Defendants violated Cal. Bus. & Prof. Code § 17200 *et seq*. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

240. Defendants' "unfair" acts and practices include:

a. Defendants failed to implement and maintain reasonable security measures to protect Plaintiff's and Class Members' personal information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach. Defendants failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents and known coding vulnerabilities in the industry;

b. Defendants' failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act (15 U.S.C. § 45), California's Customer Records Act (Cal. Civ. Code § 1798.80 et seq.), and California's Consumer Privacy Act (Cal. Civ. Code § 1798.150);

c. Defendants' failure to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Defendants' inadequate security, consumers could not have reasonably avoided the harms that Defendants caused; and

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

241. Defendants have engaged in "unlawful" business practices by violating multiple laws, including the FTC Act, 15 U.S.C. § 45, and California common law.

242. Defendants' unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' personal information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members' personal information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and HIPAA;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class Members' personal information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

243. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' personal information.

244. As a direct and proximate result of Defendants' unfair, unlawful, and fraudulent acts and practices, Plaintiff and Class Members were injured and lost money or property, which would not have occurred but for the unfair and deceptive

acts, practices, and omissions alleged herein, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their personal information.

245. Defendants' violations were, and are, willful, deceptive, unfair, and unconscionable.

246. Plaintiff and Class Members have lost money and property as a result of Defendants' conduct in violation of the UCL, as stated herein and above.

247. By deceptively storing, collecting, and disclosing their personal information, Defendants have taken money or property from Plaintiff and Class Members.

248. By deceptively storing, collecting, and disclosing their personal information, Plaintiff and Class Members overpaid Defendants for services that did not include proper data security for their Private Information.

249. Plaintiff and Class Members would not have provided their Private Information to Defendants or paid Defendants money for services if Plaintiff and Class Members had known that Defendants' data security measures were inadequate to protect their Private Information.

250. Defendants acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and Class Members' rights.

251. Plaintiff and Class Members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from Defendants' unfair, unlawful, and fraudulent business practices or use of their personal information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief, including public injunctive relief.

COUNT VII

Declaratory Judgment

(On behalf of Plaintiff & the Nationwide Class)

252. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

253. Plaintiff brings this claim individually and on behalf of the Class.

254. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

255. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and PHI and whether Defendants are currently maintaining data security measures adequate to protect Plaintiff's and Class Members from further data breaches that compromise their PII and PHI. Plaintiff alleges that Defendants' data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of her PII and PHI and remains at imminent risk that further compromises of her PII and PHI will occur in the future.

256. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owe a legal duty to secure patients' PII and PHI and to timely notify patients of a data breach under the common law, Section 5 of the FTC Act, and HIPAA; and

b. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure patients' PII and PHI.

257. This Court also should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry standards to protect patients' PII and PHI.

258. If an injunction is not issued, Plaintiff will suffer irreparable injury,

and lack an adequate legal remedy, in the event of another data breach at Defendants' properties.

259. The risk of another such breach is real, immediate and substantial.

260. If another breach of Defendants' store of patient data occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

261. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to Defendants if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

262. Issuance of the requested injunction will not disserve the public interest. In contrast, such an injunction would benefit the public by preventing another data breach at Defendants [what], thus eliminating the additional injuries that would result to Plaintiff and Class Members whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and other Class Members, prays for judgment against Defendants as follows:

A. an Order certifying the Nationwide Class and California Sub-Class, and appointing Plaintiff and her Counsel to represent the Classes;

B. equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and

Class Members;

C. injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members;

D. an award of all damages available at equity or law, including, but not limited to, actual, consequential, punitive, statutory and nominal damages, as allowed by law in an amount to be determined;

E. an award of attorney fees, costs, and litigation expenses, as allowed by law;

F. prejudgment interest on all amounts awarded and

G. all such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and other members of the proposed Classes, hereby demands a jury trial on all issues so triable.

Dated: March 6, 2024

Respectfully Submitted,

/s/ John R. Parker, Jr.

John R. Parker, Jr.
California Bar No. 257761
ALMEIDA LAW GROUP LLC
3550 Watt Avenue, Suite 140
Sacramento, California 95821
Tel: (916) 616-2936
jrparker@almeidalawgroup.com